UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,077	09/09/2003	Edwin Arturo Heredia	MS1-1354US	1406

22801 7590 12/09/2008

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
GRAHAM, PAUL J	

ART UNIT	PAPER NUMBER
2426	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/658,077	HEREDIA, EDWIN ARTURO	
	Examiner	Art Unit	
	PAUL GRAHAM	2426	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10,12-16,18,19,21-27,30-38,40,42,45,46,48,49 and 51-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10,12-16,18,19,21-27,30-38,40,42,45,46,48,49 and 51-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *4/14/08* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant argues:

Cocotis does not teach "developing a link to the signature and storing the link in the web page".

The Examiner respectfully disagrees. Cocotis does teach developing a link to signature and storing, thereby determining a signature for each web page. Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62]).

Marconcini also suggests storage of signature in web content (see Marconcini, col. 23, ll. 40-67, col. 87, ll. 5-25, scrambled with signature data the content awaits descrambling for playback).

No system as in amended claim 16 is anticipated in Marconcini

The Examiner respectfully disagrees. Marconcini shows clusters are set of files grouped in logical organization (see Marconcini, abs, col. 5, l. 63-col. 6, l. 8) as well as clusters having the inherent property of sets of files grouped logically.

Marconcini shows that the start file(s) describe parameters to execute an associated application (see Marconcini, col. 83, ll. 28-52, col. 88, ll. 30-40, as helper file(s) in execution of web browser enhancement functions, as well as the inherent

property of a start file to describe information (parameters) in order to execute an application).

Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data).

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined).

And, based on new grounds of rejection; Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint).

No system as in amended claim 25 is anticipated in Marconcini

The Examiner respectfully disagrees. Marconcini suggests a security information resource file (see Marconcini, figs. 1, 2, col. 7, l. 65-col. 8, l. 10, col. 27, ll. 5-59, with cluster info metadata such as metadata digest, signature location, a clearinghouse URL where further signature verification may be done, delegate information such as a clearinghouse URL).

Marconcini suggests where the signature location is described by a link (see clearinghouse URL), as well as Cocotis shows a signature location described by link (see Cocotis, [31-33], embedded key and content (a link) disclose or describe location of signature based on match of hashed content.

Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62], including hash code of each of files).

Based on new grounds of rejection; Sudia shows the time version info describes the version of the signature file as a function of the files in the cluster (see Sudia, col. 2, ll. 53-67, operational shares define the signature as a function of the signing devices or operators representing association of files in the cluster (see Sudia, col. 8, l. 16-col. 9, l. 35, col. 28, ll. 19-36).

Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data).

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined).

And, Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint).

Policy declarations that specify... are not disclosed in cited art.

The Examiner respectfully disagrees; Arguments are moot in view of new grounds of rejection. See combination with Wall et al. (US 2002/0120939 A1).

Signature is composed of reference, keyinfo, digestvalue, signaturevalue, version number... is not disclosed in cited art

Arguments are moot in view of new grounds of rejection. See combination with *XML-Signature Syntax and Processing* document

The newly amended claim 23 is not read on by Marconcini and Cocotis.

The Examiner respectfully disagrees. In fact, Marconcini notes that if the user's request is not verifiable that said request is repudiated, denoting a restriction of access or warning (see Marconcini, col. 13, ll. 47-65). Cocotis notes that if the signature is not verified, then a warning to a user occurs as well as restricting access to the system resources (see Cocotis, [19-20], fig. 3).

The applicant's arguments have been fully considered and are not persuasive. The claims, 1-8, 10, 12-16, 18-19, 21-27, 30-38, 40, 42, 45-46, 48-49, 51-55 stand rejected.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8, 10, 31-38, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marconcini et al. (US 6834110) and Cocotis et al. (US 2002/0112162 A1).

As to claim 1, Marconcini discloses a method of signing a supplemental television content application comprising files, the method comprising (see Marconcini, col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files):

identifying at least a first portion of the files in at least one cluster (see Marconi, col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or digest algorithm description) are identified when put into BOM—first portion of the files could be any of the parts listed);

determining a cluster signature for each cluster (see Marconcini, col. 27, 42-46, each SC is signed with signatures (an encrypted digest) for parts and for the concatenation of all parts in the SC);

and developing an expression that includes the location of the signature (see Marconcini, col. 27, ll. 13-22, a BOM is used as expression to keep track of the signature and its placement),

Marconcini discloses wherein a second portion of the files comprises a web page (see Marconcini, col. 14, ll. 20-27, the clearinghouse is a website (web page) and the Electronic digital content store is a web site (web page) and they are listed in the BOM (see Marconcini, col. 27, ll. 27-45);

Marconcini is unclear on determining a signature for a webpage; however, Cocotis, who discloses a system for authentication and verification of webpage content, does teach this (see Cocotis, [0031-33]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Marconcini with the system of Cocotis in order to safeguard the content as originally stored given storage and transmission on an open network like the Internet (see Cocotis, [0027]).

By determining at least one of: developing a link to the signature and storing the link in the web page (see Cocotis, [0043] the transmission of a digital certificate is the development of link);

and storing the signature in the web page (see Cocotis, [0060-61], validation of server signature is based on signature of the web page, fig. 2, Cocotis does teach developing a link to signature and storing, thereby determining a signature for each web page. Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the

key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62]).

Marconcini also suggests storage of signature in web content (see Marconcini, col. 23, ll. 40-67, col. 87, ll. 5-25, scrambled with signature data the content awaits descrambling for playback)).

As to claim 2, Marconcini and Cocotis disclose the method of claim 1 wherein said signature for each cluster is based on a hash code of the files composing the cluster (see Marconcini col. 27, ll. 15-19).

As to claim 3, Marconcini and Cocotis disclose the method of claim 1 wherein the application comprises a start file and further comprising storing the expression in the start file, wherein the start file is a file that describes parameters to execute an associated application (see Marconcini, col. 88, ll. 30-40 and col. 83, ll. 30-40, the SC(s) processor, is a file or API that starts the application such as a web-browser using the SC(s), which contain a BOM or "the expression" within it, Marconcini shows that the start file(s) describe parameters to execute an associated application (as helper file(s) in execution of web browser enhancement functions, as well as the inherent property of a start file to describe information (parameters) in order to execute an application)).

As to claim 4, Marconcini and Cocotis disclose the method of claim 1 wherein the application comprises a start file and further comprising storing a link to the expression in

the start file (see Marconcini, col. 88, ll. 30-40 and col. 83, ll. 30-40, the SC(s) processor, is a file or API that starts the application contains the BOM which is a link to the BOM).

As to claim 5, Marconcini and Cocotis disclose the method of claim 1 further comprising storing at least one of delegate information, security policy information, time version information, and file identification information for each cluster in the expression (see Marconcini, col. 27, ll. 25-44, within the BOM (expression) an expiration date or time version info is stored as well as a description of the digest algorithm or security policy info).

As to claim 6, Marconcini and Cocotis disclose the method of claim 1 further comprising storing the cluster signature in a signature file (see Marconcini, col. 27, ll. 15-20, the BOM is a signature file for it stores the digest for an SC (or cluster)),

developing a reference to the files composing the cluster (see Marconcini, col. 25-45, the BOM is a reference for the files (or parts) in the cluster (or SC)

and storing the reference to the files in the signature file (see Marconcini, col. 27, ll. 15-20, the BOM is a signature file).

As to claim 7, Marconcini and Cocotis disclose the method of claim 1 further comprising storing the cluster signature in a signature file, developing a time version record for the cluster, and storing the time version record in the signature file (see Marconcini, col. 27, ll. 28-40, the expiration date is a time version record for the cluster (the SC) and is stored in the BOM (signature file)).

As to claim 8, Marconcini and Cocotis disclose the method of claim 1 further comprising developing at least one of a reference to the files composing the cluster, and a time version record for the cluster (see Marconcini, col. 27, ll. 25-45, the BOM is a reference to the files (parts) for the cluster (SC)).

As to claim 10, Marconcini and Cocotis disclose the method of claim 1 wherein the web pages is at least one of a markup language based application and dynamically created by a client (see Cocotis, [0013], the web page is based on HTML, a markup language).

As to claim 31, Marconcini discloses a computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising (see Marconcini, col. 64, ll. 23-47, content processing tools):

identifying at least a first portion of the supplemental television content application files in at least one cluster (see Marconi, col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or digest algorithm description) are identified when put into BOM—first portion of the files could be any of the parts listed);

determining a cluster signature for each cluster (see Marconcini, col. 27, 42-46, each SC is signed with signatures (an encrypted digest) for parts and for the concatenation of all parts in the SC);

and developing an expression that includes the location of the signature (see Marconcini, col. 27, ll. 13-22, a BOM is used as expression to keep track of the signature and its placement);

Marconcini also suggests storage of signature in web content (see Marconcini, col. 23, ll. 40-67, col. 87, ll. 5-25, scrambled with signature data the content awaits descrambling for playback)).

Marconcini discloses wherein a second portion of the files comprises a web page (see Marconcini, col. 14, ll. 20-27, the clearinghouse is a website (web page) and the Electronic digital content store is a web site (web page) and they are listed in the BOM (see Marconcini, col. 27, ll. 27-45);

Marconcini is unclear on determining a signature for a webpage; however, Cocotis, who discloses a system for authentication and verification of webpage content, does teach this (see Cocotis, [0031-33]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Marconcini with the system of Cocotis in order to safeguard the content as originally stored given storage and transmission on an open network like the Internet (see Cocotis, [0027]).

By determining at least one of: developing a link to the signature and storing the link in the web page (see Cocotis, [0043] the transmission of a digital certificate is the development of link);

and storing the signature in the web page (see Cocotis, [0060-61], validation of server signature is based on signature of the web page, fig. 2, Cocotis does teach developing a link to signature and storing, thereby determining a signature for each web page. Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62]).

As to claims 32-38, they are analyzed similar to claims 2-8, respectively (see above).

As to claim 40, it is analyzed similar to claim 10.

4. Claims 12, 15, 16, 18, 21- 25, 30, 42, 45, 46, 48-49, 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marconcini et al. (US 6834110) and Cocotis et al. (US 2002/0112162 A1) in view of Sudia (US 6209091).

As to claim 12, Marconcini discloses a method of signing a supplemental television content application comprising files, the method comprising (see Marconcini, col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files):

identifying a first portion of the files that together compose a web page (see Marconcini, col. 14, ll. 20-27, the clearinghouse is a website (web page) and the Electronic digital content store is a web site (web page) and col. 20, 41-46, the web page content or

metadata is part of content SC, they are listed in the BOM (see Marconcini, col. 27, ll. 27-45);

Marconcini also suggests storage of signature in web content (see Marconcini, col. 23, ll. 40-67, col. 87, ll. 5-25, scrambled with signature data the content awaits descrambling for playback));

Marconcini is unclear on determining a signature for a webpage; however, Cocotis, who discloses a system for authentication and verification of webpage content, does teach this (see Cocotis, [0031-33]);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Marconcini with the system of Cocotis in order to safeguard the content as originally stored given storage and transmission on an open network like the Internet (see Cocotis, [0027]);

Wherein the expression comprises at least one of security policy information data or delegate data (see Cocotis, [12, 17], delegate data is available in the expression as well as security policy information),

developing an expression that includes signature information (link to the signature) and storing the expression (link) in the web page (see Cocotis, [0043] the transmission of a digital certificate is the development of link);

and storing the signature in the web page (see Cocotis, [0060-61], validation of server signature is based on signature of the web page, fig. 2, Cocotis does teach developing a link to signature and storing, thereby determining a signature for each web page. Cocotis

denotes the graphics file (a web page) contains a link to signature, a combination of the key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62]).
Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data).

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined).

And, Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Marconcini and Cococtis with Sudia giving the authorizing agent a delegation mechanism (see, Sudia, col. 3, 38-41).

As to claim 15, it is analyzed similar to claim 1 (see above).

As to claim 22, it is analyzed similar to claim 12 (see above).

As to claim 23, Marconcini discloses a method of executing a supplemental television content application comprising files, the method comprising (see Marconcini, col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files):

Marconcini is unclear on determining if files compose web pages; however, Cocotis, who discloses a system for authentication and verification of webpage content, does teach this (see Cocotis, abstract, before receiving files requested as part of web page, the system determines the file(s) actually compose web pages by noting their registration with the server, note reading and verifying the signature).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Marconcini with the system of Cocotis in order to safeguard the content as originally stored given storage and transmission on a open network like the Internet (see Cocotis, [0027]);

and if any of the files compose web pages, then for each of the web pages, decoding the web page to determine if the web page has one of a link to a digital signature, reading the signature, and verifying the signature (see Cocotis, fig. 3, after reception the signature is verified);

if any of the web pages lack the link to a digital signature, lack the digital signature, or the signatures is not verified then warn a user that a file has not been signed, warn the user that the signature is not valid, reject the file, or restrict access by the web page to system resources (In fact, Marconcini notes that if the user's request is not verifiable that

said request is repudiated, denoting a restriction of access or warning (see Marconcini, col. 13, ll. 47-65). Cocotis notes that if the signature is not verified, then a warning to a user occurs as well as restricting access to the system resources (see Cocotis, [19-20], fig. 3).

As to claim 16, Marconcini discloses a method of executing a supplemental television content application that comprises files, the method comprising (see Marconcini, col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files):

determining if the files are arranged in a cluster, wherein a cluster is a subset of the files grouped through logical organization, and determining if any of the files are arranged in clusters comprises: (see Marconcini, col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or content or digest algorithm description) are determined a part of a cluster (an SC) when put into BOM, Marconcini shows clusters are set of files grouped in logical organization (see Marconcini, abs, col. 5, l. 63-col. 6, l. 8) as well as clusters having the inherent property of sets of files grouped logically);

for each cluster, determining the location of the signature of the cluster (see Marconcini, col. 27, ll. 20-50, the location of signature is the digest listed in the BOM which is available to receiver);

determining the files that compose the cluster (see Marconcini, col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or content or digest algorithm description) are determined a part of a cluster (an SC) when put into BOM);

and verifying the integrity of the files in the cluster by operations including verifying the signature (see Marconcini, col. 27, ll. 50-58);

determining if an application start file has a record that includes one of a reference to an expression having a location of the signature, and the expression, wherein the start file is a file that describes parameters to execute an associated application (Marconcini shows that the start file(s) describe parameters to execute an associated application (see Marconcini, col. 83, ll. 28-52, col. 88, ll. 30-40, as helper file(s) in execution of web browser enhancement functions, as well as the inherent property of a start file to describe information (parameters) in order to execute an application, as well as determining if start file has reference to location of signature (as part of all required processing of SCs);

reading from the expression the location of a file having a signature of a cluster for each cluster, wherein the reading operation further comprises reading whether there are any delegates for any of the clusters (see Marconcini, col. 83, ll. 28-52, col. 88, ll. 30-40, as helper file(s) in execution of web browser enhancement functions, as well as the inherent property of a start file to describe information (parameters) in order to execute an application, as well as determining if start file has reference to location of signature (as part of all required processing of SCs);

Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data).

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined).

And, Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint, see Sudia, fig. 5 and col. 28, ll. 19-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Marconcini and Cococtis with Sudia giving the authorizing agent a delegation mechanism (see, Sudia, col. 3, 38-41, col. 28, ll. 5-17).

As to claim 18, it is analyzed similar to claim 1 (see above).

As to claim 19, it is analyzed similar to claim 2 (see above).

As to claim 21, it is analyzed similar to claim 5 (see above).

As to claim 24, it is analyzed similar to claim 16 (see above).

As to claim 25, Marconcini discloses a supplemental television content architecture comprising (see Marconcini, fig. 5 for architecture, col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing):

An application comprising a collection of files (see Marconcini, col. 50, ll. 45-47 for application files, Col. 88, ll. 5-50);

A cluster of the files, wherein the cluster is a subset of the files grouped through a logical organization (Marconcini shows clusters are set of files grouped in logical organization (see Marconcini, abs, col. 5, l. 63-col. 6, l. 8) as well as clusters having the inherent property of sets of files grouped logically),

The files comprising:

A signature file comprising a cluster signature, a reference to the cluster, and a time version information (see Marconcini, col. 27, ll. 28-40, the expiration date is a time version record for the cluster (the SC) and is stored in the BOM (signature file));

A security information resource file comprising a cluster information metadata, a signature location metadata, and a delegate metadata (see Marconcini, figs. 1, 2, col. 7, l. 65-col. 8, l. 10, col. 27, ll. 5-59, with cluster info metadata such as metadata digest, signature location, a clearinghouse URL where further signature verification may be done, delegate information such as a clearinghouse URL); and

Marconcini shows that the start file(s) describe parameters to execute an associated application (see Marconcini, col. 83, ll. 28-52, col. 88, ll. 30-40, as helper file(s) in execution of web browser enhancement functions, as well as the inherent property of a start file to describe information (parameters) in order to execute an application, including all processing of SCs, such as link to security info file).

Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data).

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined, and cluster signature has hash code for each of the files, Cocotis [31-32]).

And, Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Marconcini and Cococtis with Sudia giving the authorizing agent a delegation mechanism (see, Sudia, col. 3, 38-41).

Wherein the time version information describes the version of the signature file as a function of the files in the cluster, and wherein the delegate metadata comprises identity and constraints of a delegate (see Sudia, col. 2, ll. 53-67, operational shares define the signature as a function of the signing devices or operators representing association of files in the cluster (see Sudia, col. 8, l. 16-col. 9, l. 35, col. 28, ll. 19-36);

Wherein the delegate metadata comprises identity of a delegate (see Marconcini, col. 9, l. 60-col. 10, l. 15, use of clearing house or electronic store denotes identity of delegate).

As to claim 30, it is analyzed similar to claim 5.

As to claim 42, Marconcini discloses a computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising(see Marconcini, col. 64, ll. 23-47, content processing tools):

identifying a first portion of supplemental television content application file that together compose a web page (see Marconcini, col. 14, ll. 20-27, the clearinghouse is a website (web page) and the Electronic digital content store is a web site (web page) and they are listed in the BOM (see Marconcini, col. 27, ll. 27-45);

Marconcini also suggests storage of signature in web content (see Marconcini, col. 23, ll. 40-67, col. 87, ll. 5-25, scrambled with signature data the content awaits descrambling for playback));

Marconcini discloses wherein a second portion of the files comprises a web page (see Marconcini, col. 14, ll. 20-27, the clearinghouse is a website (web page) and the Electronic digital content store is a web site (web page) and they are listed in the BOM (see Marconcini, col. 27, ll. 27-45);

Marconcini is unclear on determining a signature for a webpage; however, Cocotis, who discloses a system for authentication and verification of webpage content, does teach this (see Cocotis, [0031-33]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Marconcini with the system of Cocotis in order to safeguard the content as originally stored given storage and transmission on an open network like the Internet (see Cocotis, [0027]).

By determining at least one of: developing a link to the signature and storing the link in the web page (see Cocotis, [0043] the transmission of a digital certificate is the development of link);

and storing the signature in the web page (see Cocotis, [0060-61], validation of server signature is based on signature of the web page, fig. 2, Cocotis does teach developing a link to signature and storing, thereby determining a signature for each web page. Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the

key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62]);

developing an expression that includes signature information (link to the signature) and storing the expression (link) in the web page (see Cocotis, [0043] the transmission of a digital certificate is the development of link);

and storing the signature in the web page (see Cocotis, [0060-61], validation of server signature is based on signature of the web page, fig. 2, Cocotis does teach developing a link to signature and storing, thereby determining a signature for each web page. Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62]).
Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

As to claim 45, it is analyzed similar to claim 1.

As to claim 46, Marconcini discloses a computer readable media having stored thereon a plurality of instructions that, when executed by at least one processor, causes the processor to perform acts comprising (see Marconcini, col. 5, ll. 61-65 for method,

col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files):

determining if any supplemental television content application files are arranged in a cluster (see Marconcini, col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or content or digest algorithm description) are determined a part of a cluster (an SC) when put into BOM, Marconcini shows clusters are set of files grouped in logical organization (see Marconcini, abs, col. 5, l. 63-col. 6, l. 8) as well as clusters having the inherent property of sets of files grouped logically));

for each cluster, determining the location of the signature of the cluster (see Marconcini, col. 27, ll. 20-50, the location of signature is the digest listed in the BOM which is available to receiver);

determining the files that compose the cluster (see Marconcini, col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or content or digest algorithm description) are determined a part of a cluster (an SC) when put into BOM);

and verifying the integrity of the files in the cluster by operations including verifying the signature (see Marconcini, col. 27, ll. 50-58);

and determining if any of the files are arranged in clusters comprises: (see Marconcini, col. 5, ll. 5-45, a cluster (an SC) of files (parts such as metadata or clearinghouse URL or content or digest algorithm description) are determined a part of a cluster (an SC) when put into BOM, Marconcini shows clusters are set of files grouped in logical organization

(see Marconcini, abs, col. 5, l. 63-col. 6, l. 8) as well as clusters having the inherent property of sets of files grouped logically);

for each cluster, determining the location of the signature of the cluster (see Marconcini, col. 27, ll. 20-50, the location of signature is the digest listed in the BOM which is available to receiver);

determining if an application start file has a record that includes one of a reference to an expression having a location of the signature, and the expression, wherein the start file is a file that describes parameters to execute an associated application (Marconcini shows that the start file(s) describe parameters to execute an associated application (see Marconcini, col. 83, ll. 28-52, col. 88, ll. 30-40, as helper file(s) in execution of web browser enhancement functions, as well as the inherent property of a start file to describe information (parameters) in order to execute an application, as well as determining if start file has reference to location of signature (as part of all required processing of SCs);

reading from the expression the location of a file having a signature of a cluster for each cluster, wherein the reading operation further comprises reading whether there are any delegates for any of the clusters (see Marconcini, col. 83, ll. 28-52, col. 88, ll. 30-40, as helper file(s) in execution of web browser enhancement functions, as well as the inherent property of a start file to describe information (parameters) in order to execute an application, as well as determining if start file has reference to location of signature (as part of all required processing of SCs);

Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider).

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data).

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined).

And, Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint, see Sudia, fig. 5 and col. 28, ll. 19-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Marconcini and Cococtis with Sudia giving the authorizing agent a delegation mechanism (see, Sudia, col. 3, 38-41, col. 28, ll. 5-17).

As to claims 48, 49, 51, and 52they are analyzed similar to claims 18, 19, 21, and 22, respectively (see above).

As to claim 53, Marconcini discloses a method of executing a supplemental television content application comprising files, the method comprising (see Marconcini,

col. 5, ll. 61-65 for method, col. 12, ll. 45-48 for metadata, see abstract and title for TV content, see col. 15, ll. 34-36 for signing and col. 50, ll. 45-47 for application files):

Marconcini is unclear on determining if files compose web pages; however, Cocotis, who discloses a system for authentication and verification of webpage content, does teach this (see Cocotis, abstract, before receiving files requested as part of web page, the system determines the file(s) actually compose web pages by noting their registration with the server, note reading and verifying the signature).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Marconcini with the system of Cocotis in order to safeguard the content as originally stored given storage and transmission on a open network like the Internet (see Cocotis, [0027]);

and if any of the files compose web pages, then for each of the web pages, decoding the web page to determine if the web page has one of a link to a digital signature, reading the signature, and verifying the signature (see Cocotis, fig. 3, after reception the signature is verified);

if any of the web pages lack the link to a digital signature, lack the digital signature, or the signatures is not verified then warn a user that a file has not been signed, warn the user that the signature is not valid, reject the file, or restrict access by the web page to system resources (In fact, Marconcini notes that if the user's request is not verifiable that said request is repudiated, denoting a restriction of access or warning (see Marconcini, col. 13, ll. 47-65). Cocotis notes that if the signature is not verified, then a warning to a

user occurs as well as restricting access to the system resources (see Cocotis, [19-20], fig. 3).

As to claim 54, it is analyzed similar to claim 16.

As to claim 55, Marconcini discloses a supplemental television content architecture comprising (see Marconcini, col. 27, ll. 5-25):

an application comprising a collection of files (see Marconcini, col. 29, ll. 25-40); the files comprising :

wherein the signature changes as the web page changes (see Marconcini, col. 29, l. 58-col. 30, l. 12),

Marconcini suggests a security information resource file (see Marconcini, figs. 1, 2, col. 7, l. 65-col. 8, l. 10, col. 27, ll. 5-59, with cluster info metadata such as metadata digest, signature location, a clearinghouse URL where further signature verification may be done, delegate information such as a clearinghouse URL, a link).

Marconcini suggests where the signature location is described by a link (see clearinghouse URL), as well as Cocotis shows a signature location described by link (see Cocotis, [31-33], embedded key and content (a link) disclose or describe location of signature based on match of hashed content.

Cocotis denotes the graphics file (a web page) contains a link to signature, a combination of the key, hash, and content (see Cocotis, [31-33]). The signature data stored with page data (see Cocotis, [31-33], embedded), for each file (see Cocotis, [85], as well as at least a link to signature embedded with use of public key, see Cocotis, [60-62], including hash code of each of files);

Marconcini shows that a delegate is an entity authorized to sign or verify an event (see Marconcini, col. 3, ll. 5-59, an inherent property of a delegate is its authorization to verify in addition to a main signer, an electronic store vis-à-vis the content provider);

Marconcini shows determining a delegate name and constraints, wherein constraint comprises time boundaries (see Marconcini, col. 9, l. 60-col. 10, l. 15, such as use of a clearing house or electronic store for distribution of time limited or licensed data);

Additionally, Cocotis teaches delegation of verification authority (see Cocotis [30], fig. 1, secure transaction authority server is example) where said delegate name and constraints are determined);

And, Sudia, who discloses a digital signature system, teaches delegation of verification authority (see col. 2, l. 48-col. 3, l. 43, determining a delegate and time constraint);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Marconcini and Cococtis with Sudia giving the authorizing agent a delegation mechanism (see, Sudia, col. 3, 38-41).

5. Claims 13, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marconcini et al. (US 6834110) and Cocotis et al. (US 2002/0112162 A1) in view of Sudia (US 6209091) in view of XML-signature Syntax and Processing (NPL, March 2002).

As to claim 13, Marconcini , Cocotis, and Sudia disclose the method of claim 12, wherein the metadata is extensible markup language metadata (see Cocotis, [13], the document markup language is extensible, the metadata is therefore, extensible markup language (as further evidenced by use of RFC3275);

The combination of Marconcini , Cocotis, and Sudia are unclear on a syntactical extension of an extensible markup language link; however the use of XML-signature Synatx and processing document, which illustrates use of XML as metadata (see instant specification as well), does show a syntactical extension of markup language link with linkage between XML doc and signature (see XML-signature Synatx and processing document, p. 61, 69, use of XLink).

The manual also shows elements that compose a signature:

Ref element – p. 8
Keyinfo element – p. 8
Digestvalue element – p. 8
Signaturevalue element – p. 8
versionNumber element – p. 9, serial number used in processes, uses signature properties and represents a version number under separate namespace
making use of SignatureProperties element – p. 4

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Marconcini , Cocotis, and Sudia with XML-signature Synatx and processing document in order to give definition signature processing in light of XML usage (see XML-signature Syntax and Processing, abstract).

As to claim 27, it is analyzed similar to claim 13.

6. Claims 14, 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Marconcini et al. (US 6834110) and Cocotis et al. (US 2002/0112162 A1) in view of Sudia (US 6209091) in view of Wall et al. (US 2002/0120939 A1).

As to claim 14, Marconcini , Cocotis, and Sudia disclose the method of claim 12, and Marconcini teaches security policy information (see Marconcini, col. 27, ll. 25-44, within the BOM (expression) an expiration date or time version info is stored as well as a description of the digest algorithm or security policy info); however the combination is unclear on location of permission request file and privacy statement;

Wall, who discloses a webcasting system, does teach security policy information data that comprises specifying a location of a permission request file or privacy statement (see Wall, [52], FAQs are permission files and privacy statement links specify location of docs).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Marconcini , Cocotis, and Sudia with that of Wall in order to direct the user to documents useful for security information via a consistent navigation scheme (see Wall, [52]).

As to claim 26, it is analyzed similar to claim 14.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Inquiries

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul J. Graham whose telephone number is 571-270-1705. The examiner can normally be reached on Monday-Friday 8:00a-5:00p EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vivek Srivastava can be reached on 571-272-7304. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

pjg

12/3/2008

/Vivek Srivastava/

Supervisory Patent Examiner, Art Unit 2426